Cisco Virtualized Multi-Tenant Data Center, Version 2.x

Last Updated: November 3, 2011

Cisco Validated Design

Building Architectures to Solve Business Problems

Cisco Virtualized Multi-Tenant Data Center, Version 2.x

Introduction

The Cisco Virtualized Multi-Tenant Data Center (VMDC) solution 2.x provides design and implementation guidance for enterprises planning to deploy private cloud services and service providers building virtual private and public cloud services. The Cisco VMDC 2.x solution integrates various Cisco and third-party products that are part of the cloud computing ecosystem.

This document includes the following topics:

Solution Overview

Cisco VMDC 2.x is a validated architecture that delivers a highly available, secure, flexible, and efficient data center infrastructure. It provides the following benefits:

- Reduced time to deployment—Provides a fully tested and validated architecture that accelerates technology adoption and rapid deployment.
- Reduce risk—Enables enterprises and service providers to deploy new architectures and technologies with confidence.
- Increased flexibility—Rapid, on-demand, workload deployment in a multi-tenant environment due to a comprehensive automation framework with portal-based resource provisioning and management capabilities
- Improved operational efficiency—Integrates automation with multi-tenant resource pool (compute, network, and storage), improves asset use, reduces operational overhead, and mitigates operational configuration errors.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Differences between Cisco VMDC 2.x and VMDC 1.1

Cisco VMDC 2.x is the second phase of Cisco's Virtualized Multi-Tenant Data Center solution. The details of the first phase of the solution (VMDC 1.1) are described at:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/landing_vmdc.html

Table 1 summarizes the high level differences:

Table 1 Comparison of VMDC 1.1 and 2.x

VMDC 1.1	VMDC 2.x
Generic virtualized multi-tenant data center architecture	Standardized data center architecture employing pre-integrated compute stacks, such as Vblock and FlexPod
Focus on design for infrastructure components of data center (compute, storage, network)	Focus on infrastructure components and automation (including service orchestration)
Single design applicable for various data center sizes	Two standardized designs based on data center size (compact and large)

Architecture Overview

Modular Design

Cisco VMDC 2.x provides a scalable solution that can address the needs of smaller, as well as larger, enterprise and service provider data centers. This architectural consistency enables providers to select the design that best suits their immediate needs, while providing a solution that can scale to meet future needs without re-tooling or re-training staff. This scalability with a hierarchical design based on two modular building blocks: PoD and ICS.

Point of Delivery (PoD)

The modular design starts with a basic infrastructure module called a PoD. A PoD allows providers to add network, compute, and storage resources incrementally. The Cisco VMDC 2.x architecture specifies two PoD designs: Compact and Large.

The PoD concept offers a number of benefits:

- Predefined logical units
- Simplified capacity planning
- Ease of new technology adoption
- Fault isolation
- Consistent and efficient operation

Integrated Compute Stack (ICS)

The second building block in Cisco VMDC 2.x is a generic Integrated Compute Stack (network, storage, and compute) based on existing models, such as the VCE Vblock and Cisco-NetApp FlexPod offerings. The VMDC 2.x architecture is not limited to a specific ICS definition but can be extended to include other compute and storage stacks. Both enterprises and service providers can build and deploy their ideal cloud platform using the ICS design, implementation, and operational best practices described in the Cisco VMDC 2.x documentation.

The ICS benefits include the following:

- Pre-validated physical units
- Simplified capacity planning
- Ease of new technology adoption
- Fault isolation
- Consistent build out and operation
- Flexible and efficient resource allocation

Multi-Tenant Support, Separation, and Security

Multi-tenancy refers to the virtualization of network, storage, and compute resources across the data center for each tenant. In VMDC 2.x, logical separation is used instead of requiring dedicated physical resources for each tenant. This separation is a critical attribute of any cloud deployment, as it differentiates cloud computing from co-location and dedicated infrastructure for each application.

Some of the virtualization technologies are Multi-VRF, multi-context Cisco Application Control Engine (ACE) and Cisco Catalyst 6500 Series Firewall Service Module (FWSM), and the Nexus 1000V. Table 2 presents the features and technologies that enable a layered security strategy in Cisco VMDC.

Table 2 Layered Security Strategy

Layer	Security Options
Data Center Edge	• Secured access and perimeter firewall • Multiprotocol Label Switching (MPLS) Layer 2 and 3 VPNs • SSL and IP Security (IPsec) VPNs • Infrastructure security to protect device, traffic plane, and control plane
Core and Aggregation	• Device virtualization for control-, data-, and management-plane segmentation • Infrastructure security to protect device, traffic plane, and control plane
Services	• Server load balancing to mask servers and applications • Infrastructure security to protect device, traffic plane, and control plane

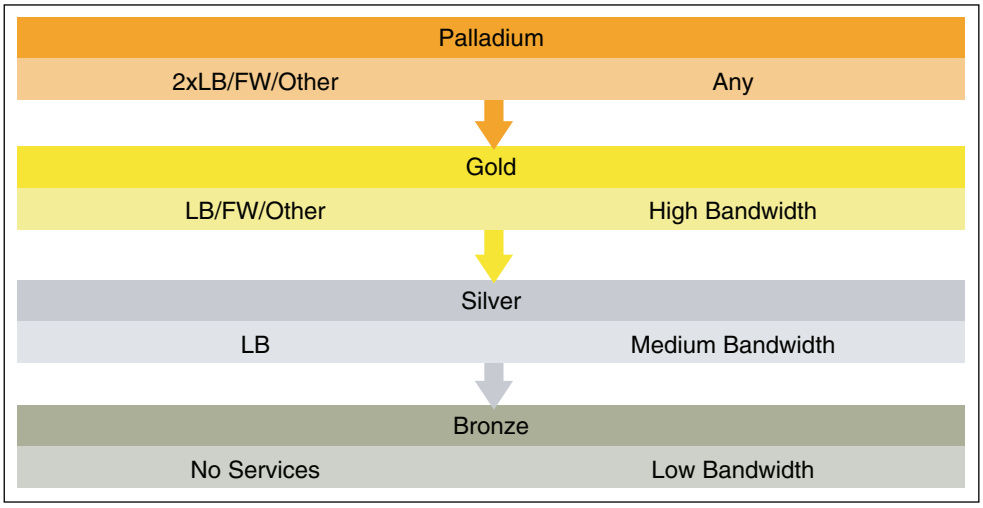
Table 2 Layered Security Strategy (continued)

Layer	Security Options
Aggregation and Access	• Secure, authenticated connections • Dynamic Address Resolution Protocol (ARP) inspection • Dynamic Host Configuration Protocol (DHCP) snooping • IP source guard • Zone security (private VLANs, port switching, and port profiles with access control lists [ACLs]) • Infrastructure security to protect device, traffic plane, and control plane
Virtual Access	• Policy-based virtual machine connectivity • Mobile virtual machine security and network policies • Virtual firewall integration with Cisco Nexus 1000V Switch
Compute	• Application security
Storage and storage aggregation	• Virtual service domains plus NetApp vFilers (NAS) • Zoning

Differentiated Services

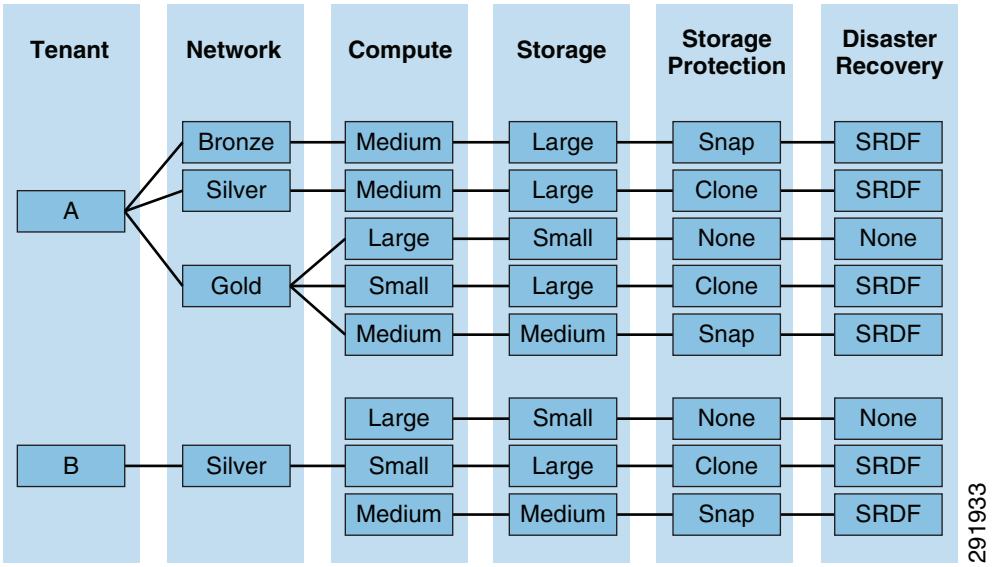
The Cisco VMDC architecture allows providers to build service level agreements (SLAs) that support their tenant or application requirements. Figure 1 is not meant to be a strict definition of resource allocation, but to demonstrate how differentiated service tiers could be built.

Figure 1 Example VMDC Service Tiers



VMDC extends service policies across the data center infrastructure allowing cloud administrators to create virtual data center addressing the specific business and application requirements of each tenant. Figure 2 is an example of two tenant virtual data centers and the possible combination of infrastructure services.

Figure 2 Example Virtual Data Center Service Policies



Service Orchestration Integration

The Cisco VMDC 2.x architecture includes an open management framework that enables provisioning of resources through service orchestration. A provider can deploy orchestration tools that provide a portal-based configuration model where a tenant can select from a defined number of service options.

Service orchestration offers a number of benefits:

- Significantly reduces the OpEx associated with administering and monitoring virtualized resources
- Decreasse provisioning time
- Provides an audit trail for fulfillment assurance and billing
- Connects and automates work flows when applicable to deliver a defined service

The service orchestrator used in the Cisco VMDC 2.x architecture is BMC Atrium Orchestrator. The overall components that enable orchestration in Cisco VMDC version 2.0 are listed in Table 3.

Table 3 Example Service Orchestration Components

Layer	Functional Element	Description
Orchestration		
	BMC AO	End-to-end service provisioning
Resource		
	BMC Atrium	Central repository for all inventory and resource details
Element management		
	UCS Manager	Configuration/monitoring tool for USC components and service profiles
	BMC BBSA	Server provisioning tool

Table 3 Example Service Orchestration Components (continued)

Layer	Functional Element	Description
	WMware vCenter	Virtual server provisioning tool
Network Management		
	CA NetQoS	Performance management
	CIC(NetCool)	Fault management and service visibility
	NaviSphere	Storage management
Service Management		
	CIC(NetCool)	Service impact and root cause determination
	BMC BBNA	Network change management and compliance
	NetQoS	Service performance
	P-NET/SLM	Monitoring
	API	Integration through multiple APIs
	BMC Remedy	Service Desk Function
	BMC Service Catalog	Central repository for all service definitions and instances
	BMC Service Portal	The user portal for ordering and administering services
	BMC Atrium CMDB	Atrium Configuration Management Database
Security		
	Cisco ACS	Authentication, authentication, and accounting
Identity		
	Active Directory	Identity repository

Cisco VMDC 2.1 uses the BMC Cloud Lifecycle Management (CLM) solution to provide a comprehensive set of capabilities for orchestrating and managing cloud environments. Table 4 describes the BMC components validated with the VMDC 2.1 architecture.

Table 4 VMDC 2.1 Validated BMC CLM Components

CLM Component
BMC Cloud Lifecycle Management
BMC Remedy Action Request System
BMC Atrium CMDB
BMC Atrium Core
BMC Bladelogic Server Automation
BMC Bladelogic Network Automation

Workload Mobility and Disaster Recovery Capability

The VMDC architecture facilitates movement of workloads from ICS to ICS within a PoD, from ICS to ICS in different PoDs, and to an ICS in a different data center. VMware Site Recovery Manager provides disaster recovery by enabling movement of workloads from one data center site to another. On the storage side, different service tiers are provided disaster recovery and data protection with customized remote replication, such as recovery-point objective (RPO) or recovery-time objective (RTO).

Compact and Large PoD Details

VMDC 2.x provides two PoD design models: Compact and Large PoDs. Each model addresses different scale, growth, and cost points. The Compact PoD targets small to medium data centers and Large PoD targets data centers with higher scale requirements. In each of the designs, multiple ICSs scale the PoDs. The data center can scale to a larger number of tenants, applications, or workloads by adding PoDs.

Table 5 highlights differences between the PoD designs.

Table 5 Differences Between Compact and Large PoD Designs

Compact PoD	Large PoD
• Applicable for small to medium data centers • Top of Rack (ToR) access design • Split VDC design (VMDC 2.0) • Single VDC design (VMDC 2.1) • 10-Gbps and 1-Gbps ICS	• Applicable for medium to larger data centers • End of Row (EoR) access design • 10-Gbps ICS

Components

Table 6 lists the components of the Cisco VDMC architecture.

Table 6 Components of the Cisco VDMC 2.x Architecture

Features	Compact PoD	Large PoD
Network	• Cisco Nexus 5020, and 7010 Switches • Cisco Catalyst 6500 Series Switches and Catalyst 6509-E (WAN edge) • Data center services node: Cisco Catalyst 6509-E Switch (Virtual Switching System [VSS]) • Cisco Nexus 2148T Fabric Extender	• Cisco Nexus 7010 , and 7018 Switches • Cisco Catalyst 6500 Series Switches and Cisco CRS-1 Modules (WAN edge) • Data center services node: Cisco Catalyst 6509-E Switch (Virtual Switching System [VSS])
Compute	• Cisco Unified Computing System • Cisco UCS 5108 Blade Server Chassis • Cisco UCS B200 M1 Blade Server • Cisco UCS M71KR-E Emulex Converged Network Adapter • Cisco UCS M81KR Virtual Interface Card • Cisco UCS 6120XP 20-Port Fabric – Cisco UCS C200-M1 – Cisco UCS 6120XP 20-Port Fabric Interconnect and Cisco UCS 6140XP 40-Port Fabric Interconnect	• Cisco Unified Computing System • Cisco UCS 5108 Blade Server Chassis • Cisco UCS B200 M1 Blade Server • Cisco UCS M71KR-E Emulex Converged Network Adapter • Cisco UCS M81KR Virtual Interface Card • Cisco UCS 6120XP 20-Port Fabric Interconnect and Cisco UCS 6140XP 40-Port Fabric Interconnect
Virtualization	• VMware vSphere • VMware ESXi 4.x Hypervisor • Cisco Nexus 1000V (virtual access switch)	• VMware vSphere • VMware ESXi 4.x Hypervisor • Cisco Nexus 1000V (virtual access switch)
Security	• Cisco Catalyst 6500 Series FWSM and Cisco ACE • VMware vShield • NetApp vFiler and Virtual Service Domains • Cisco Nexus 1000V Switch	• Cisco Catalyst 6500 Series FWSM and Cisco ACE • Cisco ASA 5580-40 • VMware vShield • NetApp vFiler and Virtual Service Domains • Cisco Nexus 1000V Switch

Table 6 Components of the Cisco VDMC 2.x Architecture (continued)

Features	Compact PoD	Large PoD
Storage fabric and arrays	• Cisco MDS 9506 and MDS 9513 Multilayer Directors and Cisco MDS 9148 and 9134 Multilayer Fabric Switches • EMC Symmetrix V-Max with virtual provisioning • NetApp FAS3170 and NetApp FAS6080	• Cisco MDS 9506 and MDS 9513 Multilayer Directors • EMC Symmetrix V-Max with virtual provisioning • NetApp FAS3170 and NetApp FAS6080
Orchestration and management	• BMC Atrium Orchestrator • VMware vCenter • Cisco UCS Manager • BMC BladeLogic for server and network • BMC Remedy IT Service Management Suite	• BMC Atrium Orchestrator • VMware vCenter • Cisco UCS Manager • BMC BladeLogic for server and network • BMC Remedy IT Service Management Suite

Solution Validation

Testing Scope

Table 7 Solution Validation Scope

Use Case	Details
Data center end-to-end functionality verification for SAN and NAS designs	End-to-end feature/integration validation including QoS for all data center network layers from access to WAN edge on all platforms. ESX/VM provisioning, boot up and maintenance, as well as SAN/NAS storage design verification.
Disaster recovery scenario validation	Transparent movement of data center workloads for business continuance (active-backup scenario).
Automation validation	Validation of service orchestration, portal, service catalog validation with element manager integration for compute and network.
Data center services functionality validation	Validation of Service Tier offerings with Data Center Services Node (firewall, load balancing)
Failover scenario validation	Validation of redundancy designs (with Baseline Steady State traffic)—Routing, vPC/MEC, ECMP, VSS, HSRP, Active-Active service modules, Clustering.
Security validation	End-to-end security validation on various components
Scalability verification	Multi-dimensional scalability (VLAN, MAC, HSRP, routes, contexts, VM) within scope of architecture

Compact and Large PoD Scale

Table 8 Validated Scalability

Feature	Compact PoD	Large PoD
Tenants	32	152
Servers per PoD	64	512
Virtual machines per PoD	1,440	11,520
VLANs per PoD	180	520
Virtual firewall contexts	6	8
Virtual load balancers	16	24
Server VLANs	180	200
MAC addresses	12,000	24,000
HSRP gateway instances	196	504
Routing protocol scale	256 OSPF neighbors	480 BGP peers

Further Reading

This document introduces the VMDC 2.02.x design. For the detailed design and implementation guides for this solution, please visit:

Cisco Virtualized Multi-Tenant Data Center, Version 2.1 Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.1/design_guide/vmdc21DesignGuide.html

Cisco Virtualized Multi-Tenant Data Center, Version 2.1 Implementation Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.1/implementation_guide/vmdc21ImplementationGuide.html

Cisco Virtualized Multi-Tenant Data Center, Version 2.0, Large Pod Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.0/large_pod_design_guide/Large_Pod_Design_Guide.pdf

Cisco Virtualized Multi-Tenant Data Center, Version 2.0, Compact Pod Design Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.0/design_guide/vmdcDesignGuideCompactPoD20.html

Cisco Virtualized Multi-Tenant Data Center, Version 2.0, Compact Pod Implementation Guide (Login Required)

http://www.cisco.com/en/US/partner/docs/solutions/Enterprise/Data_Center/VMDC/2.0/implementation_guide/vmdcImplementationGuideCompactPod20.html

Cisco Virtualized Multi-Tenant Data Center, Version 1.1

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/1.1/vmdcDg11.html

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, visit www.cisco.com/go/designzone.